REMARKS

Claims 2 and 18 have been amended. No new matter has been entered. Upon entry of the above amendments, claims 2-14 and 16-21 will remain in the application.

Claim Rejections – 35 U.S.C. §112

Claims 2 and 18 stand rejected under 35 U.S.C. §112, second paragraph, in that the language "the results of pattern matching by analyzing means of other agents" is allegedly indefinite and lacking antecedent basis. Claims 2 and 18 have been amended to obviate this rejection by reciting that the comparison includes "comparing the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by other agents to identify similar patterns of suspicious activity in different portions of the computer network." This language is believed to be more clear and clearly supported by the specification. Withdrawal of the ejection of claims 2 and 18 under 35 U.S.C. §112, second paragraph, is solicited.

Claim Rejections – 35 U.S.C. §103(a)

Claims 2-14 and 16-21 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable as obvious over Rowland (US 6,405,318) in view of Baker (US 6,775,657). This rejection is believed to be improper and is traversed.

The claimed invention relates to a system and corresponding method for detecting the state of a computer network. As set forth in amended claim 2, the system includes:

agents disposed in said computer network, each said agent comprising:

data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network;

means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said network in a normal state and activities of said network in an abnormal state; and

means for comparing collected data to said activity models to determine the state of said computer network at different times and to dynamically update said activity models,

wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network.

Claim 18 recites a corresponding method of detecting the state of a computer network. Such a system and method is not taught or suggested by Rowland.

As noted in the previous amendment response, Rowland discloses an intrusion detection system that monitors a computer system in real-time to identify activity indicative of attempted or actual access by unauthorized persons or computers. The occurrence of false alarms is purportedly reduced by comparing the user's behavior to the user's profile and known attack patterns and automatically taking action when an event (anomaly) is identified. The user's profile is dynamically updated during each use and saved. In the main embodiments, the intrusion detection system is implemented in software on a host computer. In the embodiment of Figure 9, the system further includes a central controller in a network that contains multiple host computers 151-153. Each host computer 151-153 includes the monitoring software and sends information about log auditing, login anomaly detection, etc. to the central controller for centralized auditing of events 154, data analysis 155, cross-correlation of intrusion activity throughout the network 156, and alerting the network system administrator 157 if anomalous activity is found. However, other than the paragraph at column 8, lines 8-23, Applicant can find no further detail regarding the operation of the embodiment of Figure 9.

In the Official Action, the Examiner acknowledged that Rowland does not teach comparing "the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network" as claimed. For such teachings, the examiner alleges that one skilled in the art would have looked to the teachings of Baker to modify the system of Rowland in order to determine if a specific node can be trusted. Applicant disagrees.

Baker teaches an intrusion detection system and method in which a registry is maintained of each host node address associated with a host node operable to perform intrusion detection services. The system monitors activity on the network, compares characteristics of the monitored activity with the registry, and determines from the comparison results whether the monitored activity has the characteristics in common with any of the nodes in the registry. If so, the monitored activity is dismissed as permitted activity. Importantly, and contrary to the examiner's allegations, Baker nowhere discloses comparing "the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network" as claimed. On the contrary, the detected activity in Baker is compared to a registry of a host node to determine if the activity is permitted and, if so, the network activity is dismissed and allowed to proceed unencumbered to the registered host node; otherwise, the intrusion detection services are performed at the receiving host node. Baker nowhere suggests that pattern analysis is conducted by multiple agents in a network so that patterns of suspicious activities at different portions of the computer network may be determined. The examiner's conclusions to the contrary are not supported by the teachings of Baker.

Accordingly, even if the teachings of Baker could have been used to modify the system of Rowland as the examiner suggests, the claimed system and method for providing network level coordination of the detection of suspicious activities would not have been suggested to one skilled in the art. On the contrary, the result would have been a registration system of the type taught by Baker which, as noted above, does not suggest how to identify patterns of suspicious activities at different portions of the computer network as claimed. Withdrawal of the rejection of claims 2-14 and 16-21 as being unpatentable as obvious over Rowland in view of Baker is thus proper and is respectfully solicited.

Conclusion

For the reasons set forth herein, the amendments to claims 2 and 18 are believed to place all claims in condition for allowance. A Notice of Allowability is solicited.

Date: November 3, 2008

/Michael P. Dunnam/
Michael P. Dunnam
Registration No. 32,611

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439